E29 P128EP AB/ej 03-06-25

Title:
AN ARRANGEMENT AND A METHOD RELATING TO PROTECTION OF END USER DATA

TECHNICAL FIELD

The present invention relates to an arrangement and a method respectively for protection of end user data, more generally of end user personal profile data in a communication system comprising a number of end user stations and a number of service/ information/content providers.

STATE OF THE ART

End user personal profile data tends to get more and more spread out at different locations e.g. on Internet. With the fast development of global data communication networks, it gets possible to distribute data both via fixed and via wireless applications. Data will also be pushed out to an even higher extent than hitherto, e.g. from companies to end users, other companies etc. Internet end users, mobile as well as non-mobile, have to rely on and trust service providers. The service providers, in turn, require that the end users provide a lot of personal information in order to be able to serve the end users properly, and possibly for other reasons. However, the personal information can easily be misused, consciously or unconsciously, but still very little is done to protect the privacy rights of the end users. This is a serious problem. This will also have as a consequence that fewer end users sign up to, or take advantage of, all services that could be useful for them, which also is disadvantageous. The need for means to protect privacy therefore increases. For the individual end user it is exceedingly important that his personal information can be protected from uncontrolled

distribution among service providers, other end users, companies etc. At the same time as, for example, the number of services that can be provided to end users, over for example Internet, increases, it becomes more and more interesting for service and information providers to be able to obtain detailed information about users. This may be in conflict with the security (e.g. privacy) aspect for the end users, as well as it of course also may be attractive for the end users, since they can also take advantage of personal information being spread out, and thereby obtain other useful or desired information etc. For statistical purposes it is interesting for e.g. companies to get information in order to become familiar with the needs for services, products etc. An end user may today have stored personal profile data of different kinds, at different locations, which contains various kinds of information about the user, such as name, address, particular habits, hobbies, accounts, financial situation etc. Thus, it is exceedingly important for the service/content providers to know the characteristics of existing and potential customers to allow for targeted advertising etc., at the same time as it is also exceedingly important for the end user to be able to properly protect the personal profile data.

Thus there is an inherent conflict between different interests. Therefore laws and regulations have been created in an increasing number of countries, such as for example within the European Union, to restrict the accessibility to privacy information. Such laws and regulations often vary from one country to another, but generally they have in common that the consumer or the end user should have control over his or her profile, including conditions for its release.

Solutions have been suggested for systems for protecting user personal profile data acting as a kind of a safe or functioning as

a profile repository. The profiles can, by replacement of the user identity, for example the mobile phone number, through a code, be stored such that there will be no connection to the user identity, throughout the network. Such a repository or storing means for user profiles can be arranged at different nodes within the network. One example relates to a profile holding means provided between a portal and an advertising node. It is then supposed that the personal profile has been transferred to the advertising node, with the user identity in the form of a mobile phone number (MSISDN) replaced by a code, which is totally unrelated to the phone number. The procedure will then be that the portal requests an advertisement for a user, e.g. with a phone number. The profile holding means then forwards the request to the advertising node with the mobile phone number converted into a corresponding code. The advertising node subsequently returns the advertisement to the personal profile holding means, which subsequently returns the advertisement to the portal. Such a system is for example known under the trademark Respect ™ which is an e-business platform enabling privacy control, identity management and instant personalization for on-line transactions. The profile holding means is then represented by the Respect ™ server which is a virtual infrastructure located at the mobile Internet provider.

However, there are several problems associated with systems as described above. One main issue is the transactional capacity of the profile protecting means. Normally the number of users that can be handled is limited, which results in serious problems for real time applications. With reference to the example given above, advertisements have to be served when an end user actually visits a particular page, or accesses a particular service, and many operations are time-critical. The time criticality is particularly important in wireless environments.

It is certain that complete protection of end user personal profile data can never be guaranteed, any solution can in principle be cracked by a malicious partly, but the suggestions made so far leave a lot to desire.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide an arrangement and a method respectively through which end user personal (profile) data can be protected to a high extent, particularly as much as required by most end users still wanting to make use of, and take advantage of, available services. It is also an object of the invention to provide an arrangement that makes it possible for an end user to trust a service provider to such an extent that the service provider is allowed to use personal data e.g. for statistical and other purposes while still providing the end user with the satisfaction that the data hardly can be abused of.

Further yet it is an object to provide a solution through which end user data can be provided by the end user to such an extent that also the service provider can use the data to an extent so as to be able to optimally serve the end user. It is particularly an object to provide a solution through which an agreement can be established between end user and service provider which is very difficult to break. It is a general and main object of the invention to provide an arrangement and a method respectively which make abuse of personal data extremely difficult and unlikely to happen and such that the end user can feel confident when giving away personal data.

Therefore an arrangement and a method having the features of the independent claims are suggested. Advantageous implementations are given by the appended sub-claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will in the following be more thoroughly described, in a non-limiting manner, and with reference to the accompanying drawings, in which:

Fig. 1 is a schematical block diagram illustrating the inventive concept,

Fig. 2A is a block diagram describing one implementation of the inventive concept,

Fig. 2B is a block diagram describing another implementation of the inventive concept,

Fig. 3 is a communication diagram illustrating the flow of messages according to a first implementation,

Fig. 4 is a diagram illustrating the flow of messages according to second embodiment,

Fig. 5 is a diagram illustrating the flow of messages indicating four different implementations,

Fig. 6 describes the procedure illustrating the use of a protection server, and

Fig. 7 is a flow diagram describing one implementation of the inventive concept.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 is a general overview of a basic implementation of the inventive concept. The arrangement comprises an intermediary proxy

server 2 supporting a first communication protocol for end user station (user agent) 1 communication. Intermediary proxy server 2 is in one embodiment within the personal environment of the end user, e.g. a home PC. In an alternative embodiment it is located within an intranet. According to still another embodiment it is located at the operator's premises. The intermediary proxy server also supports a second communication protocol for communication with a protection server 4.

In one implementation a certificate of the protection server 4 is registered at a trusted third-party, such as the operator having sold it and protection server certificates are somehow made available to the intermediary proxy server 2. The task of the intermediary proxy server is to verify the genuinity of a protection server 4 for example through requesting a certificate and, in a particular implementation, signed content from the protection server 4 over the second communication protocol and comparing it with published certificates stored in certificate storing means 3. It should be clear that the verification of the genuinity (e.g. authenticity) of the protection server can also be done in other manners by the intermediary proxy server.

The first communication protocol may be a secure protocol but it is not necessary for the functioning of the inventive concept. Also the second communication protocol may be a secure protocol, e.g. IPSec or HTTPS but it is also not necessary. Both the first and the second communication protocols can be so called secure protocols but neither of them has to be it, alternatively one of them, either the first or the second, may be a secure protocol. Any variation is in principle possible. The protection server 4 is in one implementation a HTTP proxy comprising a database 5 with tables holding information according to the relevant policy in order to be able to provide the service provider with what is

needed and available according to the policy. The protection server comprises a query API (Application Programming Interface) in order to allow for queries or questions being asked to the database. The protection server further comprises a simple administration API so that an IP number can be set and such that changes can be made to the privacy policy files of the service provider. When the protection server 4 is purchased, in one implementation, its certificate is registered, as referred to above, at a trusted third-party. The protection server 4 communicates with the service provider over a third communication protocol, e.g. HTTP.

In one implementation the end user preferences are held in the intermediary proxy server 2. However, in an alternative implementation the user preferences are held at the end user station. Still further the end user preferences may be agreed upon with the user klicking through them. After the negotiation they can be cached or stored such that the agreement can be handled quicker at a subsequent time. No change wanted may for example mean OK. In general the protection server should provide an API giving the service provider the possibility to change the policies of sites and pages taking the level of privacy into consideration, such that if for example the level of privacy is raised, the affected data should be deleted etc. Furthermore the protection server 4 must provide responses upon request to the intermediary proxy server 2, e.g. as far as certificates, possibly signatures etc. are concerned. Furthermore it should provide responses to requests for agreements relating to policy files and/or natural language statements to the intermediary proxy server 2. Still further it provides a query API to which questions can be asked by the service provider according to the policy settings.

Fig. 2A shows, in a somewhat more detailed manner, one implementation of the inventive concept. It is here supposed that the intermediary proxy server 2A is in communication with holding means holding published certificates 3A. The end user station here comprises a PC 1A sending requests to the intermediary proxy server using HTTP(S). The functioning is the same as above. The protection proxy server 4A comprises storing means with three tables or three separate databases DB1 $5A_1$, DB2 $5A_2$, DB3 $5A_3$. It should be clear that the number of tables is not limited to three but any relevant number of tables or separate holding means can be implemented; different tables in one and the same database relates to one implementation.

The protection proxy server 4A has an SQL allowing questions to be asked to the data base(es) $5A_1, 5A_2, 5A_3$ from the service provider (application) 6A. (It should be clear that SQL merely constitutes one example among others, e.g. LDAP (Lightweight Directory Access Protocol). It is supposed that the intermediary proxy server 2A requests a certificate and signed content from the protection proxy server 4A over an IPSec connection (or some other connection), verifies that the certificate belongs to a protection proxy server with the trusted third-party, by comparing the requested certificate with the published certificates available from certificate holding means 3A, which may be actual holding means, or over Internet or in any other manner. It is actually not necessary to implement any handling of certificates, a list of protection servers may also be available over Internet, for example. It is also supposed that, in this implementation, the intermediary proxy server 2A performs a P3P (Platform for Privacy Preferences Project) agreement, which specifies a protocol that provides an automated way for users to gain control over the use of personal data on visited web-sites. The invention covers security communication agreements in general, e.g. P3P, national

language agreements etc. used within the field of privacy. According to that web-sites are enabled to express their privacy practices in a machine readable XML (Extensible Markup Language) format that can be automatically retrieved and compared with an end user's privacy preferences. This makes it possible for an end user to make a decision as to submit or not a piece of personal information to a particular web-site. As referred to above, the user's preferences may be in the intermediary proxy server 2A or in the end user device PC 1A or agreed upon as the end user klicks them through. Storing or cashing may be implemented or not as also discussed above. After performing the P3P agreement, if the genuinity of the protection server etc. has been established, the actual web-page may be requested with the full or acceptable profile of the user. Actually also personal data such as name, address etc. can be sent since the protection server can be trusted to handle the data correctly and in a manner acceptable to the end user.

As referred to above the protection server 4A provides an API giving the service provider the possibility to change the policies of the sites and pages and if the level of privacy is raised, the affected data should be deleted. In addition to responding to requests for certificates and signatures, the protection server 4A responds to requests for P3P reference and policy files and/or natural language statements. According to the policy settings, the service provider may then ask questions over the SQL API to the protection server according to the policy settings, for example relating to user specific data such as name, address, purchased items etc., which then can be retrieved, since the protection server is trustworthy. It may also be possible to retrieve profile information, in particular implementations with history information. Further yet the service provider may retrieve

statistical data, however, in such a manner, that a specific end user cannot be tracked.

In a particular implementation statistical information and profile information is pseudonymized and anonymized in an appropriate manner, e.g. it may be stored and retrieved using a oneway hash function to ensure privacy and security also in case the protection server actually is broken into or similar.

Particularly the protection server requests the certificate and the signature from the service provider 6A. The protection proxy server 4A may pseudonymize a request (over HTTP) over the URL (Uniform Resource Locator) of the service provider. A new pseudo (e.g. a counter) has to be used for each new URL that is requested. The data that the policy file claims to use, must be sent along with the request. Particularly the protection server assures that personal data is not passed on in such a way that the profile information can be tied to the user. If for example a page wants to store some kind of user specific data, the user identity provided with the request is used to store the information in the protection server. When information is to be retrieved, however, it is important that the request comes from a page where profile information was not retrieved, in order to ensure security (the desired degree of privacy according to the policy).

Fig. 2B is a figure similar to that of Fig. 2A, but implemented for an end user station comprising a WAP (Wireless Application Protocol) device 1B instead. Then WSP (Wireless Session Protocol) is used, secure version or not. Intermediary proxy server 2B functions similar to intermediary proxy server 2A described above. It is here supposed that published certificates are held in certificate holding means 3B associated with intermediary proxy server. Particularly the intermediary proxy server and the holding

means for published certificates are at the operators premises. This is however not necessarily the case, see Fig. 2A etc. Also between the intermediary proxy server and the protection proxy server WSP (secure or not) is used. In other aspects the functioning is similar to that described with reference to Fig. 2A.

Fig. 3 is a diagram describing the communication between user agent (end user station), intermediary proxy server, protection server and application according to one implementation. It is here supposed that a request is sent from the user agent (which is not required to have any specific intelligence) to the intermediary proxy server, e.g. an ISP (Internet Service Provider). The intermediary proxy server sends a request for a certificate to the protection server, receives it and verifies it as explained above (not all steps explicitly indicated in the figure). The request is then forwarded to the protection server. Subsequently a decrypted request is sent to the application which responds with a file to the protection server. The response is forwarded to the intermediary proxy server and from there on to the user agent. SQL queries (e.g.) from the application to the protection server and responses thereto are indicated with dashed lines since it is intended to indicate that such may be provided or not, the main thing being that such a functionality is enabled and if none, one, or more such queries are actually sent, is irrelevant as long as the possibility is open to the application, or the service provider.

Fig. 4 illustrates another embodiment in which a request is sent from the user agent to the intermediary proxy server, which then sends a request for an agreement reference file to the protection server. The latter then returns an agreement reference file to the intermediary proxy server. Subsequently the intermediary proxy

server requests an agreement policy from the protection server which returns an agreement policy, a protection server indicator and a certificate. Subsequently the intermediary proxy server sends an encrypted (with the certificate) request to the protection server which forwards said request (decrypted) to the application. SQL queries are, like in the preceding figure, indicated through dashed lines. The application server provides a response with the requested file, which via the protection server and the intermediary proxy server, is returned to the user agent. The requests for agreement reference file and agreement policy etc. can be sent from the intermediary proxy server without the user agent being involved but, as indicated through the dashed lines, the user agent may also be involved, i.e. having intelligence and functionality to handle such requests. Alternatively this is handled transparently for the user agent, which does not comprise any particular intelligence or software for such actions. If the policy is changed to a lower level, data should be deleted.

Fig. 5 is also a diagram illustrating the communication between user agent, intermediary proxy server, protection server and application server. Depending on whether, here, P3P is implemented or not or if certificate verification is implemented or not, one or more of steps I, II, III, IV are implemented. In a first implementation it is supposed that P3P is implemented as well as certificate verification and that the user agent comprises a certain intelligence. Thus a P3P reference file request is sent from the user agent to the intermediary proxy server, which forwards the request to the protection server. The protection server then returns a P3P reference file to the intermediary proxy server, which in turn returns it to the user agent. (Step I)

Subsequently the user agent sends a P3P policy request, which is forwarded from the intermediary proxy server to the protection server, which then returns a P3P policy and a protection server indicator indicating the specific protection server and a certificate. This response is forwarded from the intermediary proxy server to the user agent. This corresponds to step II. A verification of this certificate is then performed, as a request to that effect is received in the intermediary server to the protection server, step III. Finally user data encrypted with the certificate is sent from the user agent via the intermediary proxy server to the protection server, e.g. according to the method as described in the patent application "Method for limiting conveyance information of user profile within mobile Internet transactions" filed in the US on August 23, 2001, which herewith is incorporated herein by reference. A decrypted request is then sent on to the application which responds with a file to the protection server and the file is subsequently returned to the user agent via the intermediary proxy server, step IV. SQL queries (V), i.e. queries from the application to the protection server can be sent to and responded to according to the policy settings and privacy settings as explained above.

In another implementation it is supposed that P3P is not implemented. Then only steps III, IV are used. In still another implementation it is supposed that the certificate verification is omitted, actually relying on the protection server being "genuine". In that case only steps I, II and IV are implemented, and still supposing that P3P is implemented. Finally the user agent may be unaware of the protection server and P3P and thus sends a request to the application. In particular this is a request with user data. (Simple requests from the user agent i.e. without user data are illustrated in Figs. 3,4). In order to be able to send user data along with the request this presupposes an

"intelligent" user agent as referred to above, which is capable of introducing data in the request. The data information is then introduced directly in the header (CC/PP, HTTP header). This is actually based on the user agent fetching the policy, cf. the patent application referred to above, XML is used and via XML tags information is acquired about which data that is needed and the relevant policy. The user agent then reads the policy, establishes what is needed and sends the relevant data straight away, which is extremely advantageous.

The US patent application referred to generally relates to a method for contacting an origin server from a user, by generating a minimal user profile for the user, which profile contains user designated CPI (Capabilities and Preferences Information). (CPI is represented through a profile and determines how far and to what extent to communicate profile information to other web sites). A connection is then established with the origin server using the minimal user profile. It is determined if a privacy policy of the origin server at least meets the privacy preferences of the user, and a second profile (at least one) containing a more detailed CPI is provided to the origin server if the privacy policy of the origin server at least meets the privacy preferences of the user. This concept, may be used in the implementation of the present inventive concept.

It should be noted that the user agent and the intermediary proxy server both can be at the operators environment, i.e. a combined entity, but this is not necessarily the case.

Fig. 6 illustrates the procedure as from the point when a decrypted request is sent from the protection server to the application. The request is particularly a HTTP request, at least containing HTTP information such as IP number etc. If the concept

described in Fig. 5 is implemented (user data in header), also such data is included. Further yet, if the request actually is a response to a form defining the required information GET/POST parameters are included (WSP or HTTP GET, POST request).

The protection server with its logic is then responsible for storing data according to agreement, or according to the policy, in the database(s) inside the protection server, or associated with the protection server. This is done in an anonymized and pseudonymized manner. The anonymized, pseudonymized HTTP request is also forwarded to the application, e.g. containing a sequence number or anything that makes it "identifiable". SQL requests for data may then be sent from the application to the protection server (storing means), and responses are provided according to the policy. Finally a HTTP response is provided to the protection server (logic part), which forwards it to the user agent via the intermediary proxy server.

Fig. 7 is a very schematic flow diagram relating to one of the implementations as disclosed in Fig. 5, and according to which P3P is implemented but no certificate verification. It is also supposed that the user agent has a particular intelligence, that the user agent has fetched the policy as indicated by means of XML tags specifying the policy and indicating what data actually is needed such that user data can be sent directly from the user agent (encrypted with the certificate).

Thus, a request for a P3P reference file is sent from the user agent via the intermediary proxy server to the protection server, 100. From the protection server the P3P reference file is then returned, 101. Subsequently a P3P policy request is sent from the user agent to the protection server, 102. The protection server then returns the P3P policy, an indication of the protection

server and a certificate to the user agent, 103. Although in this implementation no certificate verification is illustrated, a step might here be included according to which the user agent requests that the intermediary proxy server provides for a verification of the certificate or more generally of the protection server, e.g. as explained earlier in this document, which then returns a response to the user agent. With, or without, verification of the certificate, user data is then sent in the header encrypted by means of the certificate from the user agent to the protection server, 104. The protection server (logic) then provides for appropriate storing in the protection server storing means according to the policy, anonymized and pseudonymized, 105. An anonymized and pseudonymized HTTP request is also sent to the application, 106. SQL requests can then be sent from the application to the protection server, or to the storing means thereof, which then responds according to the policy, 107. Finally a response with the file is sent from the application, via the protection server etc. to the user agent, 108.

The invention is of course not limited to the explicitly illustrated embodiments, but it can be varied in a number of ways within the scope of the appended claims.